

## Off the Grid

Jul 28th, 2008 by [sherri](#)



I felt like the luckiest girl at [HOPE](#) when bernieS handed me a pair of TriSquare Digital Two-Way Radios (TSX300), a prize given away at his excellent talk, “Off the Grid - Voice/Data Communications” (Skip Arey and bernieS).

Ever since the “warrantless wiretapping” [FISA Amendments Act](#) was passed by Congress a few weeks ago, I’ve been itching to find some practical voice communication system which isn’t trivially monitored by the government. I admit that, like many security professionals, part of me had become a little resigned to the prospect of an Orwellian future (present?) Little did I expect that someone would hand me a great short-range solution at the conference.

The TSX300 radios are awesome for a number of reasons. They’re based on Frequency Hopping Spread-Spectrum (FHSS) technology, meaning that rather than broadcasting on a static frequency, they constantly switch between many frequencies. This makes it very difficult to eavesdrop on the signal, and it also means that interference on one frequency has little impact on the overall quality of the communication.

Interestingly, the use of frequency hopping for communications privacy was pioneered by Hollywood actress [Hedy Lamarr](#) and composer George Antheil, who patented their “Secret Communication System” in 1942. Their invention used a piano roll to hop between 88 frequencies, and was “intended to make radio-guided torpedoes harder for enemies to detect or jam.” (*Wikipedia*)



Up until now, radios available to the general public have lacked privacy and suffered from severe channel overcrowding. According to bernieS’ excellent March 2008 article in [Popular Communications](#), the TSX300 radios address both those issues, as follows:

The user chooses a 10-digit channel code. *“Depending on which 10-digit channel code is chosen, an embedded pseudorandom number generator algorithm selects a different set of 50 [out of 700 possible] frequencies to hop and cycle through every 20 seconds. Each 400-millisecond hop frame contains both voice and data... Since FHSS can effectively create a nearly unlimited number of ‘virtual’ radio channels (by using many different hopping sequences), it could solve the severe channel overcrowding and privacy problems vexing tens of millions of... radio users.”*<sup>1</sup>

Genius! My favorite part of the article is a section called [“Two-Way Radio Privacy For the Paranoid”](#) (who, me?) Here’s a snippet:

*“Arguably, TriSquare’s eXRS technology might offer the general public more short-range [communications security] than landline or cellular/PCS network phone calls, which can now be remotely and instantly monitored by many people at local, state and federal government agencies, thanks to CALEA (Communications Assistance for Law Enforcement Act) and the PATRIOT act.*

*“... An eXRS channel code is somewhat like a simple encryption key with 10 billion (10<sup>9</sup>) permutations... Neither scanners nor other manufacturers’ two-way radios can receive eXRS’ FHSS radios signals—further reducing the likelihood of interception. The characteristic of FHSS that rapidly slices and scatters a signal to appear as noise across a wide swath of radio spectrum makes it inherently difficult to track and demodulate. Still, if you’re really paranoid, you should know that a well-equipped and determined eavesdropper could use a highly specialized surveillance receiver like the WJ-8654 Microceptor to track and demodulate eXRS’ FHSS radio signals. More affordable fast-sweeping receivers such as those from Optoelectronics aren’t quite fast enough to track and demodulate a 400-msec FHSS signal.”*

In short, the TSX300 radios offer a practical short-range alternative to our centralized telecommunications infrastructure, which is controlled by a few corporations and tapped by the government. The TSX300 radios also support text messaging, address books and all that useful day-to-day stuff that make normal people happy.

I highly recommend reading both of bernieS’ excellent [Popular Communications](#) articles on the topic:

[Digital Two-Way Radio Technology Reaches Consumer Market](#) (Bernard Bates, November 2007)

[An Innovative License-Free Alternative to FRS/GMRS](#) (Bernard Bates, March 2008)

...and I’m totally psyched to try out my new radios at Defcon next week!

#### Footnotes:

<sup>1</sup>Bernard Bates, “An Innovative License-Free Alternative to FRS/GMRS,” Popular Communications, March 2008

<sup>2</sup>Bernard Bates, “Two-Way Radio Privacy For the Paranoid,” Popular Communications, March 2008

Sherri Davidoff